コンピュータセキュリティ 17－3
（２００２．５．２３）

1 人複数投票可能な電子投票に関する一考察

――株主総会における議決権行使プロトコルの実現――

税所哲郎[†]　齊藤泰一[‡]　土井洋[*]　辻井重男[*]

[†]中央大学・FNT　[‡]NTT 研究所　[*]中央大学研究開発機構

株主総会における議決権行使は, 各株主が所有株式数に比例した投票権を持つことから, 1 人で複数投票可能な投票とみなすことができる. しかし, 現状では, 郵送等によって行使されるため電子化は進んでおらず, セキュリティが確保されているとも言いがたい. 我々は, 株主総会の電子化を検討しているが, このためには議決権行使の電子化は不可欠である. 本稿では, 1 人で複数投票可能であるという条件に注目し, それによる問題点等を分析する. 更に, 電子議決権行使に対応できる 1 人複数投票可能な電子投票プロトコルを提案し, その評価を行う.

キーワード: 1 人複数投票, 株主総会, 電子投票

Note on Voting Schemes Suitable for Multiple Ballots per Voter

― To Construct Electronic Decision Systems at Stockholder's Meetings ―

Tetsuro SAISHO[†], Taiichi SAITO[‡], Hiroshi DOI[*], Shigeo TSUJII[*]

[†]Chuo University, FNT　[‡]NTT Labs　[*]RDI, Chuo University

Since any stockholder has ballots the number of which is proportional to his amount of stocks, the voting procedure in the annual stockholder's meeting can be seen as a modification of usual voting in democratic meetings. However the computerization of the procedures in stockholder's meetings and its security technologies have not been developed enough. We have studied the computerization in stockholder's meetings, in which the proposal of electronic decision systems at stockholder's meetings is one of our main purposes. In this paper, we focus on the property that one stockholder can vote several ballots in a stockholder's meeting, and consider related issues. Moreover we propose electronic voting schemes for stockholder's meetings through which that property holds, and clarify their benefits.

Key Words: Multiple Ballots per Voter, Stockholder's Meeting, Electronic Voting Schemes

1. 背景

株主総会における議決権行使は, 経営方針に関する議案を決定する, 会社にとって重要な意思決定手段である. 議決権行使とは一種の投票であり, 直接参加, 郵送及び委任状による代理参加により行使されるのが現状である. しかし, その電子化は進んでおらず, セキュリティが確保されているとも言いがたい. 我々は株主総会の電子化を検討しているが, 議決権行使の電子化は不可欠である.

議決権行使は, 株主の所有株式数に比例して行えるので, 1 人複数投票可能な投票とみなすことができる. 一方, 電子投票プロトコルは, 各投票者が平等に 1 票の投票権を持つという状況に対して設計される場合が多い. 従って, 1 人複数投票可能という状況に対しては, 実現は可能であるが, 効率がよいとはいえない.

そこで, 本稿では 1 人で複数投票可能であるという条件に注目し, それによる問題点等を分析する. 更に, 電子議決権行使に対応できる 1 人複数投票可能な電子投票プロトコルを提案し, その評価を行う.

以下, 第 2 章で株主総会と議決権行使の現状を述べ, 電子化のためのモデル化を行う. 更に, 1 人複数投票可能という条件による問題点等を分析する. 第 3 章で用語と記号の説明をした後, 第 4 章で方式を提案し, 評価を行う.

2. 株主総会における議決権行使

本章では, 株主総会における議決権行使の現状を示し, 電子化の際の問題点を示す.

2.1 株主総会と議決権行使

株主総会は, 会社の決算期の3ヵ月以内に開催することが, 商法[1 2]234 条及び 224 条の 3 により定められている. 日本の場合, 会社の決算期が 3 月に集中しているため, 株主総会は 6 月に集中して開催される. しかも, 多くの会社の株主総会は同一日に開催される. 従って, 1 人の株主が複数の会社の株主総会に参加するのは困難な状況である. なお, 株主総会において議決権を行使する場合は,

(1) 株主総会に出席し行使する方法,
(2) 郵送により行使する方法,
(3) 委任状により代理人が行使する方法

が提供されるので, 複数の会社に対して議決権を行使する場合は, (2)または(3)を利用することになる. なお, 株主総会に出席し議決権を行使する場合, 投票結果を判断するのは, 通常は「発声」や「拍手」の数である.

議決権行使の際, 株主は議案ごとに議決権を行使することができる. 議案ごとの投票内容は簡潔であり, 図 1に示すように, 議案に対する賛否, 賛成時の除外事項等である.

株主番号 123456	議決権行使株式数 200		
第 1 号議案	賛	否	
第 2 号議案	賛[ただし を除く]		否
第 3 号議案	賛	否	

図 1 議決権行使書の例

なお, 議決権行使株式数とは, 株主が投票できる票数であり, 株主の所有株式数から

$$\lfloor \text{所有株式数}/\text{単元株数} \rfloor \cdot \text{単元株数} \quad (1)$$

と計算できる. なお, 単元株数とは, 会社が各々定めた株式の売買単位である. 所有株式数が 240, 単元株数が 100 の場合は, 議決権行使株式数は 200 となる.

議決権行使株式数だけ賛否の投票が可能であることから, 大株主(所有株式数が多い株主)の投票全体に与える影響は大きい. 例えば, 会社の発行株式数の 30%を所有する大株主は, 事実上, 会社の経営方針を決定できる.

また, 商法 239 条の 4 により, 株主の議決権不統一行使(例えば議決権行使株式数のうち, 30%は賛成, 70%は反対とする議決権行使)は可能である. しかし, 事前申請が必要であること, 会社側で拒否できること等から, 個人株主による不統一行使は, 事実上不可能とみなされる.

議決権行使結果, 特に郵送による議決権行使書は商法 239 条に従って, 株主総会実施後 3 ヶ月は閲覧又は謄写が可能である. また, 株主なら誰でも閲覧･謄写が可能であることから, 事実上, 議決権行使結果は開示されていると考えてよい. ただし, 数万通の議決権行使書(はがき)から特定の個人の議決権行使書を探すのは困難である.

一方, 商法(会社法)に定められているように, 議案は, 株主総会において株主により議決されなくてはならない. 近年のネットワーク環境の発達を考えると, 株主にとって安全で, 利用しやすい電子的な議決権行使方式が提供されれば, 株主総会への出席者が増えることになり, 会社と株主の双方に与える恩恵は非常に大きい.

なお, 会社は株式に関する業務を行わない場合が多い. その場合, 株主情報を信託銀行に提供して, 信託銀行が株式に関する業務を代行する. 特に, 議決権行使の場合は, 議決権行使書の発行を信託銀行が代行することが多い(図 2). なお, 会社によっては議決権行使の集計までを信託銀行が代行する場合もある.

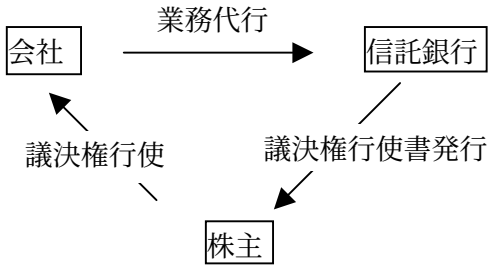

図 2 議決権行使の流れ

2.2 議決権行使の規模

2.1節で示したように, 議決権行使株式数は, 株主の「所有株式数」と「単元株数」で決まる. 表 1に, いくつかの会社の単元株数と, 発行株式総数を示す.

表 1 単元株数と発行株式総数

会社	単元株数	発行株式総数
A	1	16,134,000
B	10	25,364,000
C	100	3,649,997,000
D	1000	5,709,424,000

(1)式より, 議決権行使は, 単元株数単位で行われることがわかる. 従って, 発行株式数を単元株数で割ると, 議決権行使の総数がわかる. 例えば, D 社の場合, 1000 株を 1 票とみなしてよいので, 約 571 万票の投票と規模は等しくなる.

一方, 所有株式数の多い上位 10 人程度(以下, 大株主)については, 名義と所有株式数が公開されている. 表 1に示した会社について, 大株主が所有する株式の割合を表 2に示す.

表 2 大株主の所有株式数

会社	大株主の所有株式数(%)
A	45.9, 2.3, 1.4, 1.3, 1.3, 1.2, 0.9, 0.9
B	8.4, 6.3, 5.9, 4.0, 3.4, 3.3, 2.3, 2.2
C	5.3, 5.0, 4.2, 4.2, 4.0, 3.9, 3.9, 3.1
D	3.8, 3.7, 2.6, 2.1, 2.1, 1.8, 1.7, 1.5

B,C,D の各社では, 筆頭株主(最大株式所有者)でも, 全体の 10%に満たない株式しか所有していない. しかし, 単元株数程度しか所有していない株主と比較して, 数万倍以上の投票権を持つことから, 議決権行使に与える影響が大きいことがわかる. しかも, 所有株式数が大きいことから, 投票内容と投票者を関連付けることも可能である. 例えば, A 社の場合, 投票全体の 45.9%の投票内容が全く同じ場合は, 「A 社の筆頭株主の議決権行使内容」を推察することが可能となる. なお, 表 1や表 2に示した情報は, 有価証券報告書や会社四季報[11]などから容易に入手することができるので, 公開情報とみなすことができる.

2.3 議決権行使実現のための要件

さて, 2.1節と2.2節での考察から, 議決権行使を電子化する際の要求事項は通常の電子投票に近いことがわかる. それに加えて, 1 人複数投票可能であること, 不統一行使を防止とすることも要件となる. 前者は議決権行使の仕組みの電子化, 後者は現行の方式(特に, 不統一行使防止)を電子化することの要求である.

なお, 投票規模は, 表 1より, 総数が 1 億以下であることがわかるので, その規模に耐え得ることも要件となる.

以上を考慮して, 本稿で実現するプロトコルは, 通常の投票方式[4][7]で求められる, 下記の条件を満足することを要件とする.

(C1) 完全性(Completeness)
不正がなければ, 投票は正しく集計される.
(C2) 無記名性(Privacy)

投票結果と投票者の関連付けができない.

(C3) 2 重投票不可能性(Unreusability)
投票者は 2 度投票することはできない.

(C4) 未登録者の投票排除(Eligibility)
登録された投票者以外は投票できない.

(C5) 公平性(Fairness)
投票に影響する途中経過が露呈しない.

(C6) 検証性(Verifiability)
投票結果が正しいことを誰もが納得できる.

更に, 議決権行使の電子化(1 人複数投票可能)という要求から, 次の要件を満たすことも必要となる.

(C7) 1 人複数投票可能であること.

(C8) 不統一行使を防止すること.

(C9) 所有株式数に関する情報が, 公開されているもの以外に新たに漏れないこと.

3. 用語と記号

議決権行使に関係するエンティティは N 人の投票者(議決権行使者)V_i, 管理者 A, 集計者 T 及び確認者である. 投票は単元株数を単位とし, $\lfloor$所有株式数／単元株数$\rfloor$を, 以下, 投票者の投票数と呼ぶ. つまり, V_i は投票内容 v_i を投票数 n_i 分だけ投票することができる. 各エンティティ間は, (盗聴可能な)通常通信路, (SSL 等を利用した)暗号通信路, (Mixnet 等を利用した)匿名通信路を使用することができる. 後者ほど実現コストが高い.

更に, 下記の暗号方式を利用する.

(1) デジタル署名[10]
投票者 V_i の署名関数を σ_i, 管理者 A の署名関数を σ_A とする. 署名($\sigma_A(\cdot), \sigma_i(\cdot)$ 等)の確認は全エンティティが可能である.

(2) ブラインド署名[3]
管理者 A のブラインド署名を得るために投票者 V_i が行う前処理を χ_A とし, ブラインド部分を解除する関数を δ_A とする. x を A に署名させたい内容, r を投票者が使用する乱数とする. $y = \delta_A(\sigma_A(\chi_A(x,r)),r)$ とすると, (x, y) が A の署名となる.

(3) 部分ブラインド署名[1][2]
管理者 A の部分ブラインド署名を得るために投票者 V が行う前処理を χ_A とし, ブラインド部分を解除する関数を δ_A とする. x を A に署名させたい内容, r を投票者が使用する乱数とし, V と A の共通情報を n とする. $y = \delta_A(\sigma_A(\chi_A(x,n,r),n),n,r)$ とすると, (x, y, n) が A の署名となる.

(4) 公開掲示板
全エンティティから参照可能であり, 集計者 T にのみ追記が許される.

(5) ビットコミットメント関数[6]
全エンティティが使用できるビットコミットメント関数 $\xi(x,r)$ が公開されている. ここで, x はコミットする内容, r は乱数である.

4. 提案方式

本章では, FOO 方式[4]の繰り返し利用方式, 及び FOO 方式に部分ブラインド署名を組み合わせる方式を示す.

4.1 FOO 方式[4]の繰り返し利用方式

投票者ごとに, 既存の電子投票方式, (FOO 方式[4])を投票数だけ繰り返す方法がもっとも簡単な実現方式である. プロトコルは登録, 投票, 集計の 3 段階から構成される. 1 人複数投票可能を実現するために必要な処理を中心に, 概要を以下に示す.

4.1.1 登録

投票者 V_i と管理者 A は投票数 n_i を共有している. n_i 回だけ以下の手順を繰り返す.

(1) 投票者 V_i は議決権内容 v_i, 乱数 k_{ij} を用い, $x_{ij} = \xi(v_i, k_{ij})$ を作成する. 次に乱数 r_{ij} を使い, $e_{ij} = \chi_A(x_{ij}, r_{ij})$ と $s_{ij} = \sigma_i(e_{ij})$ を作成し, A に (e_{ij}, s_{ij}) を通常通信路を用いて送る.

(2) 管理者 A は, まず, (e_{ij}, s_{ij}) の正当性を検証する. 次に, V_i の投票数が n_i を超えていないか確認する. 2 つの検証にいずれも合格したら, $d_{ij} = \sigma_A(e_{ij})$ を作成し, V_i に返す.

(3) V_i は, $y_{ij} = \delta_A(d_{ji}, r_{ij})$ を計算し, ブラインド署名 (x_{ij}, y_{ij}) の正当性を検証する.

4.1.2 投票

n_i 回だけ, 以下の作業を繰り返す.

投票者 V_i は匿名通信路を利用して集計者

T にブラインド署名 (x_{ij}, y_{ij}) を送る．T は，(x_{ij}, y_{ij}) の正当性を検証後，公開掲示板に掲示する．なお，掲示は，投票番号 l とのペア，(l, x_{ij}, y_{ij}) となる．

4.1.3 集計

投票締め切り後，n_i 回だけ以下の作業を繰り返す．

投票者 V_i は，(l, v_i, k_{ij}) を匿名通信路を利用して，集計者 T に送る．次に，T は，(x_{ij}, v_i, k_{ij}) の正当性を検証する．この検証に合格した場合，公開掲示板に $(l, x_{ij}, y_{ij}, v_i, k_{ij})$ を掲示する．

4.1.4 考察

FOO 方式は，(C1)〜(C6)までの要件を満足する．次に，1 人複数投票可能という要求から発生する問題点について考察する．

(C7)は，上記登録･投票･集計作業を投票数 n_i 回だけ繰り返すことにより実現できる．しかし，(C8)は，上記プロトコルでは満たすことはできない．n_i 回の投票数を有する投票者 V_i が，常に同じ投票内容 v_i に対応する登録作業を行うとは限らないからである．不統一行使を防止するためには，n_i 回の投票内容が全て同一であることを，内容を知られることなく，証明しなくてはならない．原理的にはゼロ知識証明を用いて証明可能であるが，計算コストは $O(n_i)$ となる．また，(C9)については，登録･投票･集計作業を n_i 回繰り返すことから，株主の通信状況を観察することにより，所有株式数の情報が漏れる．従って，本方式は下記の問題点がある．

(1) 投票コストが $O(n_i)$ となる．特に，大株主の負荷が大きい．
(2) 通信コストが $O(n_i)$ となることから，所有株式数の情報が漏れる．
(3) 不統一行使を防止するためには，ゼロ知識証明を用いる必要があり，そのコストは $O(n_i)$ となる．

4.2 FOO 方式[4]+部分ブラインド署名方式

本節では，FOO 方式[4]に記載された方式に部分ブラインド署名を組み合わせる方式を提案する．この方式は，4.1節で示した方式とは異なり，一度に複数投票できる．なお，一度に投票できる値はシステムで決められているものとし(本稿では 2 のべき乗)，それを投票単位と呼ぶ．V_i の投票数を $n_i = \sum n_{ij} 2^j$ とすると，$n_{ij} = 1$ となる j に対して，投票単位 2^j 分だけ投票を行う．なお，V_i の投票回数は $O(\log(n_i))$ となる．

4.2.1 登録

投票者 V_i と管理者 A は投票数 n_i を共有している．V_i の投票数を $n_i = \sum n_{ij} 2^j$ とすると，$n_{ij} = 1$ となる j に対して，以下の手順を繰り返す．

(1) 投票者 V_i は議決権内容 v_i，乱数 k_{ij} を用い，$x_{ij} = \xi(v_i, k_{ij})$ を作成する．次に投票単位 2^j，乱数 r_{ij} を使い，$e_{ij} = \chi_A(x_{ij}, 2^j, r_{ij})$ と $s_{ij} = \sigma_i(e_{ij})$ を作成し，A に $(e_{ij}, s_{ij}, 2^j)$ を暗号通信路を用いて送る．
(2) 管理者 A は，まず，$(e_{ij}, s_{ij}, 2^j)$ の正当性を検証する．次に，V_i が投票単位 2^j を未登録か確認する．2 つの検証にいずれも合格したら，$d_{ij} = \sigma_A(e_{ij}, 2^j)$ を作成し，V_i に返す．
(3) V_i は，$y_{ij} = \delta_A(d_{ji}, 2^j, r_{ij})$ を計算し，部分ブラインド署名 $(x_{ij}, y_{ij}, 2^j)$ の正当性を検証する．

4.2.2 投票

投票者 V_i は匿名通信路を利用して，集計者 T に部分ブラインド署名 $(x_{ij}, y_{ij}, 2^j)$ を送る．T は，$(x_{ij}, y_{ij}, 2^j)$ の正当性を検証後，公開掲示板に掲示する．なお，掲示は，投票番号 l とのペア，$(l, x_{ij}, y_{ij}, 2^j)$ となる．

4.2.3 集計

投票締め切り後，投票者 V_i は，(l, v_i, k_{ij}) を匿名通信路を利用して，集計者 T に送る．次に，T は，(x_{ij}, v_i, k_{ij}) の正当性を検証する．この検証に合格した場合，公開掲示板に $(l, x_{ij}, y_{ij}, 2^j, v_i, k_{ij})$ を掲示する．

4.2.4 考察

(C7)は，上記登録･投票･集計作業を繰り返すことにより実現できる．しかし，(C8)は，4.1.4 節と同様の問題が発生する．これは，ゼロ知識証明を利用して解決できる．しかも，4.1節で示した方式と異なり，そのコストは $O(\log(n_i))$ となる．(C9)については，投票者の計算コスト，通信コストは $O(n_i)$ ではなく $O(\log(n_i))$ となる．通信コストと投票数が比例しないので，通信路の観察から所有株式数を推測するのは困難とな

る. なお, 登録手続きで, 暗号通信路を用いないと, 通信中に含まれる投票単位 2^j から V_i の所有株式数に関する情報が漏れる.

一方, 投票単位を設けない場合を考えてみる. この場合, A と V_i は投票数 n_i を共有しているから, 手順(1)で投票単位 2^j を送る必要はない. 従って, 暗号通信路を使わなくて済む上, 処理･通信コストが投票数と無関係となる. しかし, 公開掲示板の内容 $(l, x_i, y_i, n_i, v_i, k_i)$ から, 大株主のように所有株式数が公開されている場合は, 投票者と投票内容を関連付けることができる. 従って投票単位を設けなくてはならない.

また, 投票単位は適切な上限を設けなくてはならない. 例えば, 投票数が 2^{20} を超える投票者が V_m のみの場合は, 投票単位が 2^{20} となる投票結果 v_m が集計後に公開されると, 投票者 V_m と投票内容 v_m の関連が付く. 投票単位の上限を, その投票単位を利用する投票者が複数いるように設定すれば, 投票単位から投票者を一意に決定することはできない.

5. まとめ

本稿で記述した, 2 種類の電子議決権行使プロトコルの特長を表 3に示す. 効率の点等から 4.2節で示した方式の優位性がわかる.

表 3 提案方式の特長

項目	4.1節	4.2節
投票者の通信コスト*	$O(n)$	$O(\log n)$
投票者の計算コスト*	$O(n)$	$O(\log n)$
集計時の計算コスト*	$O(n)$	$O(\log n)$
不統一行使防止のコスト*	$O(n)$	$O(\log n)$
必要な通信路	匿名	暗号, 匿名

*)投票者の投票数を n とした, 投票者ごとのコスト.

なお, 無証拠性[10]に関する考察や, 集計作業の改良[7], プロトコル全体としての安全性の証明を与えることは今後の課題である. また, 準同型暗号 (高次剰余暗号[5], OU 関数[8], Paillier 関数[9])を使った場合の有効性について検討する必要がある.

謝辞

本研究に関し熱心に討論いただいた辻井研究室の鈴木昭正氏に感謝します. なお, 本研究において, 土井, 辻井は TAO(通信･放送機構)の支援を一部受けました.

参考文献

[1] M. Abe, E. Fujisaki, “How to Date Blind Signatures”, K. Kim, T. Matsumoto (Eds.), ASIACRYPT’96, LNCS 1163, pp.244-251, 1996.

[2] M. Abe, T. Okamoto, “Provably Secure Partially Blind Signatures”, M. Bellare (Ed.), CRYPTO2000, LNCS 1880, pp.271-286, 2000.

[3] D. Chaum, “Blind Signatures for Untraceable Payments”, D. Chaum, R. L. Rivest, A. T. Sherman (Eds.) CRYPTO’82, Plenum Press, 1983, pp.199-203.

[4] A. Fujioka, T. Okamoto, K. Ohta, “A Practical Secret Voting Scheme for Large Scale Elections”, J. Seberry, Y. Zheng (Eds.), AUSCRYPT’92, LNCS 718, pp.244-251, 1993.

[5] K. Kurosawa, S. Tsujii, “A General method to Construct Public Key Residue Cryptosystems”, Trans. IEICE, Vol. E73, No. 7, pp.1068-1072, 1990.

[6] M. Naor, “Bit Commitment Using Pseudo-Randomness”, G. Brassard (Ed.), CRYPTO’89, LNCS 435, pp.128-136, 1990.

[7] M. Ohkubo, F. Mimura, M. Abe, A. Fujioka, T. Okamoto, “An Improvement on a Practical Secret Voting Scheme”, M. Mambo, Y. Zheng (Eds.), ISW’99, LNCS 1729, pp.225-234, 1999.

[8] T. Okamoto, S. Uchiyama, “A New Public-Key Cryptosystem as Secure as Factoring”, K. Nyberg (Ed.), EUROCRYPT’98, LNCS 1403, pp.308-318, 2000.

[9] P . Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”, J. Stern (Ed.), EUROCRYPT’99, LNCS 1592, pp.223-238, 1999.

[10] 岡本龍明, 山本博資, ”現代暗号”, 産業図書, 1997.

[11] 会社四季報 2002 年1集新春号, 東洋経済新報社, 2002.

[12] 平井宜雄, 青山善充, 菅野和夫編集代表, ”六法全書平成 14 年版”, 有斐閣, 2002.